Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 12 (2006) 638–652

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Linear error-block codes

Keqin Feng[a,*,1], Lanju Xu[a], Fred J. Hickernell[b,2]

[a] *Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China*

[b] *Department of Mathematics, Hong Kong Baptist University, Kowloon Tong, Hong Kong SAR, China*

Received 15 September 2004; revised 28 March 2005

Communicated by Gary L. Mullen

Available online 6 June 2005

Dedicated to Zhexian Wan who taught the first author algebra in 1960s and coding theory in 1970s. In the years between, Wan couldn't teach and Feng couldn't learn mathematics

Abstract

A linear error-block code is a natural generalization of the classical error-correcting code and has applications in experimental design, high-dimensional numerical integration and cryptography. This article formulates the concept of a linear error-block code and derives basic results for this kind of code by direct analogy to the classical case. Some problems for further research are raised.

Keywords: Error-block code; Linear code

1. Introduction

Let $q = p^l$ be a power of a prime number p and $\mathbb{F}_q$ be the finite field with q elements. A partition, π, of a positive integer n, is defined as

$$\pi : n = n_1 + \cdots + n_s, \quad n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s \geqslant 1, \quad s \geqslant 1.$$

* Corresponding author.

E-mail addresses: kfeng@math.tsinghua.edu.cn (K. Feng), xulj03@mails.tsinghua.edu.cn (L. Xu), fred@hkbu.edu.hk (F.J. Hickernell).

[1] Supported by a grant from the National 973 Research Project on Information Theory and NSFC, No. 60276016.

[2] Supported by the Hong Kong Research Grants Council Grant HKBU/2007/03P.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.03.006

This partition is denoted by $\pi = [n_1][n_2]\dots[n_s]$ or $[m_1]^{l_1}\dots[m_r]^{l_r}$ if

$$n_1 = \cdots = n_{l_1} = m_1 > n_{l_1+1} = \cdots = n_{l_1+l_2} = m_2 > \cdots$$
$$\cdots > n_{l_1+l_2+\cdots+l_{r-1}+1} = \cdots = n_{l_1+\cdots+l_r} = m_r.$$

Let $V_i = \mathbb{F}_q^{n_i}$ $(1 \leqslant i \leqslant s)$, and $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s = \mathbb{F}_q^n$. Each vector in V can be written uniquely as $v = (v_1, \dots, v_s)$, $v_i \in V_i$ $(1 \leqslant i \leqslant s)$.

For any $u = (u_1, \dots, u_s)$ and $v = (v_1, \dots, v_s)$ in V, we define the π-weight $w_\pi(u)$ of u and the π-distance $d_\pi(u, v)$ of u and v by

$$w_\pi(u) = \sharp\{i \,|\, 1 \leqslant i \leqslant s,\ u_i \neq 0 \in V_i\}$$

and

$$d_\pi(u, v) = w_\pi(u - v) = \sharp\{i \,|\, 1 \leqslant i \leqslant s,\ u_i \neq v_i\}.$$

An $\mathbb{F}_q$-linear subspace C of V is called a $[n, k, d]_q$ linear error-block code over $\mathbb{F}_q$ with type π, where $k = \dim_{\mathbb{F}_q} C$. Here $d = d(C)$ is the minimum π-distance of C, which is defined as

$$\begin{aligned} d &= \min\{d_\pi(c, c') | c, c' \in C,\ c \neq c'\} \\ &= \min\{w_\pi(c) | 0 \neq c \in C\}. \end{aligned}$$

The linear error-block code with $\pi = [1]^n$ reduces to the classical linear error-correcting code. The construction of linear error-block codes with the largest rate, k/n, and the minimum distance, d, is an important problem in coding theory, with applications to experimental design, high-dimensional numerical integration, and cryptography. In coding theory linear error-block codes may be used to correct errors occurring within $\leqslant (d-1)/2$ blocks. Likewise error-block codes may also be used to construct cryptographic schemes.

Linear error-block codes yield mixed-level orthogonal arrays [3], which are used for experimental design. For a $[n, k, d]_q$ linear error-block code C with type π, let M be the $q^{n-k} \times n$ matrix over $\mathbb{F}_q$ such that its q^{n-k} rows are the codewords of the dual code $C^\perp$. The matrix M may be written in block form, $[M_1, M_2, \dots, M_s]$, where each $q^{n-k} \times n_j$ block M_j has elements m_{ijk}. From this matrix M one may construct a $q^{n-k} \times s$ matrix A with elements $a_{ij} = m_{ij1}q^{n_j-1} + \cdots + m_{ij,n_j}$. The matrix A is an orthogonal array of strength $d-1$ with s factors and q^{n_j} levels for factor j. Suppose that one chooses any $d-1$ distinct columns of A, indexed by $j_1, \dots, j_{d-1}$. The fact that A is an orthogonal array means that the submatrix formed by these columns contains exactly $q^{n-k-n_{j_1}-\cdots-n_{j_{d-1}}}$ copies of every row of the form $(c_1, \dots, c_{d-1})$ with $c_k = 0, \dots, q^{n_{j_k}} - 1$. Classical error-correcting codes yield orthogonal arrays with the same number of levels per factor, thus linear error-block codes provide a more general construction of orthogonal arrays.

There is another generalization of classical error-correcting codes, called poset codes, which was initiated by Niederreiter [8] and developed by Brualdi [1], Kim [4] and Lee [5]. For poset codes the coordinates $\{1, 2, \dots, n\}$ are considered to be a partially ordered set so that the codes have a more combinatorial flavor. Linear error-block codes have

both combinatorial and algebraic behaviors. In this paper, we stress the algebraic aspect to show how many algebraic methods used in the classical case can be shifted directly to constructing good linear error-block codes.

We use standard terminologies and facts for classical linear codes which can be found in the monographs [6,7,9]. We sketch or omit proofs of some results if they are just direct analogies of the classical case.

2. Hamming and singleton bounds

Theorem 2.1. *Let C be a $[n,k,d]$ linear error-block code over $\mathbb{F}_q$ with type $\pi = [n_1],[n_2],\ldots,[n_s]$, $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s$. There exist Hamming bounds*:

$$q^{n-k} \geqslant b_\pi(l) \quad \text{for } d = 2l+1, \tag{1}$$

$$q^{n-k} \geqslant b'_\pi(l) \quad \text{for } d = 2l \geqslant 2, \tag{2}$$

where

$$b_\pi(l) = 1 + \sum_{\lambda=1}^{l} \sum_{1 \leqslant i_1 < \cdots < i_\lambda \leqslant s} (q^{n_{i_1}} - 1)\cdots(q^{n_{i_\lambda}} - 1),$$

$$b'_\pi(l) = q^{n_1}\left[1 + \sum_{\lambda=1}^{l-1} \sum_{2 \leqslant i_1 < \cdots < i_\lambda \leqslant s} (q^{n_{i_1}} - 1)\cdots(q^{n_{i_\lambda}} - 1)\right]$$

and the Singleton bound:

$$n - k \geqslant n_1 + n_2 + \cdots + n_{d-1} \quad (\Leftrightarrow k \leqslant n_d + n_{d+1} + \cdots + n_s). \tag{3}$$

Proof. For a vector $v = (v_1,\ldots,v_s) \in V = \mathbb{F}_q^n$, $v_i \in V_i = \mathbb{F}_q^{n_i}$ $(1 \leqslant i \leqslant s)$, the block-support of v is defined by

$$\mathrm{Supp}(v) = \{i \mid 1 \leqslant i \leqslant s, v_i \neq 0\}.$$

For any integer $l \geqslant 0$ and $v \in V$, the ball with center v and radius l is

$$\begin{aligned} B_\pi(v;l) &= \{u \in V \mid d_\pi(u,v) = w_\pi(v-u) \leqslant l\} \\ &= \{u \in V \mid \sharp\mathrm{Supp}(v-u) \leqslant l\}. \end{aligned}$$

For $l \geqslant 1$, we define

$$B'_\pi(v;l) = \{u \in B_\pi(v;l) \mid |\mathrm{Supp}(u-v) \cap \{2,3,\ldots,s\}| \leqslant l-1\}.$$

It is easy to see that the size of $B_\pi(v;l)$ and $B'_\pi(v;l)$ are $b_\pi(l)$ and $b'_\pi(l)$, respectively. If $d = 2l+1$, the q^k balls $B_\pi(c;l)$ with center $c \in C$ are disjoint, so that $q^n \geqslant q^k b_\pi(l)$. If $d = 2l \geqslant 2$, the q^k sets $B'_\pi(c;l)$ with $c \in C$ are disjoint, so that $q^n \geqslant q^k b'_\pi(l)$. This yields the Hamming bounds (1) and (2).

Let $H = [H_1, H_2, \ldots, H_s]$ be a parity-check matrix of the linear code C where H_i is a $(n-k)\times n_i$ block-matrix over $\mathbb{F}_q$ $(1 \leqslant i \leqslant s)$ such that for $v = (v_1,\ldots,v_s) \in V = \mathbb{F}_q^n$,

$$v \in C \Leftrightarrow Hv^\top = \sum_{i=1}^{s} H_i v_i^\top = 0 \in \mathbb{F}_q^{n-k}.$$

As in the classical case, the minimum distance of C is d if and only if

(i) the union of columns of each $d-1$ blocks are $\mathbb{F}_q$-linearly independent; and
(ii) there exist d blocks in H such that the union of the columns of these blocks are $\mathbb{F}_q$-linearly dependent.

In particular, this implies that the columns of the first $d-1$ blocks are linearly independent. Since the number of rows is $n-k$, it follows that $n-k \geqslant n_1+n_2+\cdots+n_{d-1}$. □

Definition 2.2. A linear error-block code C is called a *perfect code* if it attains the Hamming bound. It is called an *MDS code* if it attains the Singleton bound.

Example. Let $s \geqslant 2, n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s$, $n = \sum_{i=1}^{s} n_i$, $k = \sum_{i=2}^{s} n_i$ and $H = [H_1, H_2, \ldots, H_s]$ where for each i $(1 \leqslant i \leqslant s)$, H_i is an $(n-k) \times n_i$ matrix over $\mathbb{F}_q$ such that their n_i columns are F_q-linearly independent in $\mathbb{F}_q^{n-k}$ (we can do this since $n-k = n_1 \geqslant n_i$). The linear code C with parity-check matrix H is an $[n,k,2]_q$ code with type $[n_1][n_2]\ldots[n_s]$. For this code C, (2) is right: $q^{n-k} = q^{n_1}$. Thus C is perfect code.

The following result shows how to construct perfect codes and MDS codes with $d = 3$.

Theorem 2.3. *Suppose that there exists a linear code $C = [n,k,3]_q$ with type $\pi = [n_1][n_2]\ldots[n_s]$. Then $N = \frac{q^{n-k}-1}{q-1} - \sum_{i=1}^{s} \frac{q^{n_i}-1}{q-1} \geqslant 0$ and there exists a linear code $C' = [n+r, k+r, 3]_q$ with type $\pi' = [n_1][n_2]\ldots[n_s][1]^r$ provided that $0 \leqslant r \leqslant N$. Moreover, C' is a perfect code if $r = N$.*

Proof. Let $H = [H_1, H_2, \ldots, H_s]$ be a parity-check matrix of C. Then for $1 \leqslant i < j \leqslant s$, the columns of $[H_i, H_j]$ are $\mathbb{F}_q$-linearly independent in $\mathbb{F}_q^{n-k}$. By the Hamming bound we know that $q^{n-k} - 1 \geqslant \sum_{i=1}^{s} (q^{n_i} - 1)$, so that N is a non-negative integer. Since the n_i columns in H_i are linearly independent, they generate an n_i-dimensional subspace of $\mathbb{F}_q^{n-k}$ which contains $q^{n_i} - 1$ non-zero vectors. If $N \geqslant r \geqslant 1$, then $q^{n-k} - 1 > \sum_{i=1}^{s} (q^{n_i} - 1)$, so that there exists $0 \neq u_i \in F_q^{n-k}, (1 \leqslant i \leqslant r)$ such that $\{u_i\} \cup H_k$, and $\{u_i\} \cup \{u_j\}$, are linearly independent $(1 \leqslant i \neq j \leqslant r, 1 \leqslant k \leqslant s)$. Then we have $H' = [H_1, H_2, \ldots, H_s, H_{s+1}, \ldots, H_{s+r}]$ such that $H_{s+i} = u_i \in F_q^{n-k}$ and the columns of $[H_\lambda, H_\mu]$ are linearly independent for all $1 \leqslant \lambda < \mu \leqslant s+r$. Let C' be the linear code having parity-check matrix H'. Then $C' = [n', k', 3]_q$ with type $\pi' = [n_1]\ldots[n_s][1]^r$, $n' = n_1 + \cdots + n_s + r = n + r$ and $k' = n' - (n-k) = k + r$. If $r = N$, then $q^{n'-k'} - 1 = q^{n-k} - 1 = \sum_{i=1}^{s} (q^{n_i} - 1) + r(q-1)$ so that C' is perfect. □

Corollary 2.4. (i) *There exists a linear error-block code $[n,k,3]_q$ $(1 \leqslant k < n)$ with type $[n_1][n_2][1]^r$ $(n = n_1 + n_2 + r,\ r \geqslant 1)$ if and only if both the Hamming bound* (1) *and the Singleton bound* (3) *hold.*

(ii) *For any integers $m \geqslant 2$, $n_1 \geqslant n_2 \geqslant 1$ such that $m \geqslant n_1 + n_2$ and $q^m \geqslant q^{n_1} + q^{n_2}$, there exist a perfect linear code $[n_1+n_2+N, n_1+n_2+N-m, 3]_q$ with type $[n_1][n_2][1]^N$*

where $N = (q^m - q^{n_1} - q^{n_2} + 1)/(q-1)$, *and an MDS linear code* $[n_1+n_2+r, r, 3]_q$ *with type* $[n_1][n_2][1]^r$ *for each* r, $1 \leqslant r \leqslant (q^{n_1}-1)(q^{n_2}-1)/(q-1)$.

Proof. Statement (ii) is a direct consequence of (i). To prove (i) note that the Hamming and Singleton bounds,

$$q^{n-k} - 1 \geqslant (q^{n_1}-1) + (q^{n_2}-1) + r(q-1), \quad n-k \geqslant n_1+n_2, \tag{4}$$

are necessary for existence of a linear code $[n,k,3]_q$ with type $[n_1][n_2][1]^r$. On the other hand, suppose that (4) and (5) are hold, then $n_1+n_2 \leqslant n-k \leqslant n_1+n_2+r = n$ so that $n-k = n_1+n_2+t$, $0 \leqslant t \leqslant r$. We choose column vectors $u_1, \ldots, u_{n-k}$ in $\mathbb{F}_q^{n-k}$ to be linearly independent. Let $H = [H_1, H_2, \ldots, H_{t+2}]$ where $H_1 = [u_1 \cdots u_{n_1}]$, $H_2 = [u_{n_1+1} \cdots u_{n_1+n_2}]$, and $H_{i+2} = [u_{i+n_1+n_2}]$ $(1 \leqslant i \leqslant t)$. Then the linear code with parity-check matrix H is an error-block code $[n-k, 0, 3]$ with type $[n_1][n_2][1]^t$. By Theorem 2.3 there exists a linear code $[n,k,3]$ with type $[n_1][n_2][1]^r$. □

More perfect codes and MDS codes are constructed in following sections.

3. From $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$

Let $q' = q^m$ and $\{\omega_1, \ldots, \omega_m\}$ be a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q'}$. Any $a \in \mathbb{F}_{q'}$ may be expanded in terms of this basis as $a = a^{(1)}\omega_1 + \cdots + a^{(m)}\omega_m$ $(a^{(\lambda)} \in \mathbb{F}_q, 1 \leqslant \lambda \leqslant m)$. Write $\varphi(a) = (a^{(1)}, \ldots, a^{(m)}) \in \mathbb{F}_q^m$. Then $\varphi : \mathbb{F}_{q'} \to \mathbb{F}_q^m$ is a $\mathbb{F}_q$-linear isomorphism. Let $H' = (a_{ij})_{1 \leqslant i \leqslant l, 1 \leqslant j \leqslant n}$ $(a_{ij} \in \mathbb{F}_{q'})$ be any $l \times n$ matrix over $\mathbb{F}_{q'}$ whose elements satisfy the following expansion:

$$a_{ij} = \sum_{\lambda=1}^{m} a_{ij}^{(\lambda)} \omega_\lambda, \quad a_{ij}^{(\lambda)} \in \mathbb{F}_q.$$

Then, for any vector $v' = (v_1, \ldots, v_n) \in \mathbb{F}_{q'}^n$, $v_j = \sum_{\lambda=1}^m v_j^{(\lambda)}\omega_\lambda$ $(v_j^{(\lambda)} \in \mathbb{F}_q)$, we have

$$H'v'^{\top} = 0 \iff \sum_{j=1}^{n} a_{ij} v_j = 0 \quad (1 \leqslant i \leqslant l).$$

The right-hand side of this expression may be written in terms of elements in $\mathbb{F}_q$:

$$\begin{aligned} \sum_{j=1}^{n} a_{ij} v_j &= \sum_{j=1}^{n} a_{ij} \sum_{\mu=1}^{m} v_j^{(\mu)} \omega_\mu = \sum_{\mu=1}^{m} \sum_{j=1}^{n} (\omega_\mu a_{ij}) v_j^{(\mu)} \\ &= \sum_{\mu,\lambda=1}^{m} \sum_{j=1}^{n} (\omega_\mu a_{ij})^{(\lambda)} \omega_\lambda v_j^{(\mu)} \\ &= \sum_{\lambda=1}^{m} \left(\sum_{\mu=1}^{m} \sum_{j=1}^{n} (\omega_\mu a_{ij})^{(\lambda)} v_j^{(\mu)} \right) \omega_\lambda. \end{aligned}$$

Therefore the relation $H'v'^{\top} = 0$ in $\mathbb{F}_{q'}^n$ may be written as an equivalent relation in $\mathbb{F}_q^n$ as follows:

$$\begin{aligned} H'v'^{\top} = 0 &\iff \sum_{\mu=1}^{m}\sum_{j=1}^{n}(\omega_\mu a_{ij})^{(\lambda)}v_j^{(\mu)} = 0 \quad (1\leqslant\lambda\leqslant m,\ 1\leqslant i\leqslant l) \\ &\iff Hv^{\top} = 0, \end{aligned}$$

where $v = (\varphi(v_1), \varphi(v_2), \ldots, \varphi(v_n)) \in \mathbb{F}_q^{nm}$, and $H = \left[H_{ij}\right]_{1\leqslant i\leqslant l, 1\leqslant j\leqslant n}$ is an $lm \times nm$ matrix over $\mathbb{F}_q$ with $m \times m$ blocks

$$\begin{aligned} H_{ij} &= \begin{bmatrix} (\omega_1 a_{ij})^{(1)} & \cdots & (\omega_m a_{ij})^{(1)} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ (\omega_1 a_{ij})^{(m)} & \cdots & (\omega_m a_{ij})^{(m)} \end{bmatrix} \\ &= \left[\varphi(\omega_1 a_{ij})^{\top}, \ldots, \varphi(\omega_m a_{ij})^{\top}\right]. \end{aligned}$$

Let the jth column of H' correspond to the jth block of H. Then columns in H' are $\mathbb{F}_{q'}$-linearly independent if and only if the columns in the corresponding blocks in H are $\mathbb{F}_q$-linearly independent. This gives the proof of the first part of the following result.

Theorem 3.1. *Let C' be the linear code over $\mathbb{F}_{q'}$ with parity-check matrix H', and C be the linear code over $\mathbb{F}_q$ with parity-check matrix H, where H' and H are related as described above. Then*

(i) *C' is $[n, k, d]_{q'}$ code with type $\pi' = [n_1][n_2]\cdots[n_s]$ if and only if C is $[nm, km, d]_q$ code with type $\pi = [n_1 m][n_2 m]\cdots[n_s m]$*
(ii) *C' is MDS code if and only if is C MDS code. For $d = 2l+1$, C' is perfect code if and only if is C perfect code.*

Proof. Part (i) was proved above. To prove part (ii) note that

$$\begin{aligned} C' \text{ is MDS code} &\iff k = \sum_{i=d}^{s} n_i \iff km = \sum_{i=d}^{s}(n_i m) \\ &\iff C \text{ is MDS code.} \end{aligned}$$

Furthermore, for $d = 2l+1$,

$$\begin{aligned} &C' \text{ is perfect code over } \mathbb{F}_{q'} \\ &\iff q'^{n-k} = 1 + \sum_{\lambda=1}^{l}\sum_{1\leqslant i_1<\cdots<i_\lambda\leqslant s}(q'^{n_{i_1}} - 1)\cdots(q'^{n_{i_\lambda}}) - 1 \\ &\iff q^{nm-km} = 1 + \sum_{\lambda=1}^{l}\sum_{1\leqslant i_1<\cdots<i_\lambda\leqslant s}(q^{n_{i_1}m} - 1)\cdots(q^{n_{i_\lambda}m} - 1) \\ &\iff C \text{ is a perfect code over } \mathbb{F}_q. \qquad \square \end{aligned}$$

Example 1. For $q' = q^m$, there exists the Hamming code $[n,k,d]_q = \left[\frac{q'^l-1}{q'-1}, \frac{q'^l-1}{q'-1} - l, 3\right]_{q'}$ with type $[1]^n$ for any $l \geqslant 2$. By Theorem 3.1 there exists a perfect linear code $\left[m\frac{q^{ml}-1}{q^m-1}, m(\frac{q^{ml}-1}{q^m-1} - l), 3\right]_q$ with type $[m]^{\frac{q^{ml}-1}{q^m-1}}$ for any $m \geqslant 1$ and $l \geqslant 2$.

Example 2. Combining Corollary 2.4 and Theorem 3.1 yields the following results:

(i) For $m \geqslant 1$, $1 \leqslant k < n$ there exists a linear code $[nm, km, 3]_q$ with type $[n_1m][n_2m][m]^r$ $(n = n_1 + n_2 + r,\ r \geqslant 1)$ if and only if both the Hamming and Singleton bounds hold.

(ii) For any integers $l \geqslant 1$, $m \geqslant 2$, $n_1 \geqslant n_2 \geqslant 1$ such that $m \geqslant n_1 + n_2$ and $q^{ml} > q^{n_1 l} + q^{n_2 l} - 1$, there exist a perfect linear code $[(n_1+n_2+N)l, (n_1+n_2+N-m)l, 3]_q$ with type $[n_1l][n_2l][l]^N$ where $N = \frac{1}{q^l-1}(q^{ml} - q^{n_1 l} - q^{n_2 l} + 1)$ and an MDS linear code $[(n_1 + n_2 + r)l, rl, 3]_q$ with type $[n_1l][n_2l][l]^r$ for each r, $1 \leqslant r \leqslant \frac{(q^{n_1 l}-1)(q^{n_2 l}-1)}{q^l-1}$.

4. Dual codes and weight enumerators

For a linear code C in $\mathbb{F}_q^n$, there exists a dual code $C^\perp$ of C, defined by

$$C^\perp = \{v \in \mathbb{F}_q^n | (v, c) = 0 \text{ for all } c \in C\},$$

where the inner product is $(v, u) = \sum_{i=1}^n v_i u_i \in \mathbb{F}_q$ for $v = (v_1, \ldots, v_n), u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$. In the classical case, $C^\perp$ is a MDS linear code if (and only if) C is an MDS linear code. The following example shows that this may not be true in the general error-block case.

Example. Let C be a binary linear code with type $[2]^2[1]^3$ and parity-check matrix

$$H = \left[\begin{array}{cc|cc|c|c|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

This code has parameters $[n,k,d] = [7,3,3]$ and so is an MDS code ($k = n_3+n_4+n_5 = 3$). Now H is a generating matrix of $C^\perp$ so that $v = (1\,0\,0\,0\,0\,0\,0) \in C^\perp$. Thus $C^\perp = [n, k^\perp, d^\perp] = [7,4,1]$. Considering $C^\perp$ as an error-block code with the same type as C, it follows that $C^\perp$ is not an MDS code since $4 = k^\perp \neq n_1 + \cdots + n_5 = 7$.

For the particular type $\pi = [m]^s$ $(n_1 = n_2 = \cdots = n_s = m)$, we have following result, which can be proved in the same way as for the classical case.

Theorem 4.1. *Let C be a linear code $[n,k,d]_q$ with type $[m]^s$, and let G and H be the generating and parity-check matrices of C, respectively. Considering $C^\perp$ as a linear code with same type $[m]^s$ (same partition of $\{1,2,\ldots,n\}$), then the following four*

statements are equivalent to each other:

(i) *C is an MDS code*;
(ii) *$m|k$ and the column vectors from any $(n-k)/m$ distinct blocks of H are $\mathbb{F}_q$-linearly independent*;
(iii) *$m|k$ and the column vectors from any k/m distinct blocks of G are $\mathbb{F}_q$-linearly independent*; *and*
(iv) *$C^\perp$ is an MDS code.*

Definition 4.2. For a linear code $C = [n, k, d]_q$ with type $\pi = [n_1] \cdots [n_s]$, the weight enumerator of C is defined by

$$f_C(x, y) = \sum_{c \in C} x^{s - w_\pi(c)} y^{w_\pi(c)} = \sum_{i=0}^{s} A_i x^{s-i} y^i,$$

where A_i is the number of codewords c in C with π-weight i, i.e.

$$A_i = \sharp\{c \in C \mid w_\pi(c) = i\}.$$

Write $q = p^b$, a power of the prime number p. Let T be the trace mapping for $\mathbb{F}_q/\mathbb{F}_p$, and $\zeta = \zeta_p = e^{\frac{2\pi i}{p}}$. For any $u \in \mathbb{F}_q^n$, we consider the following polynomial in z:

$$g_u(z) = \sum_{v \in \mathbb{F}_q^n} \zeta^{T((u,v))} z^{w_\pi(v)}.$$

Then it follows that

$$\sum_{u \in C} g_u(z) = \sum_{v \in \mathbb{F}_q^n} z^{w_\pi(v)} \sum_{u \in C} \zeta^{T((u,v))} = q^k \sum_{v \in C^\perp} z^{w_\pi(v)}. \tag{7}$$

On the other hand,

$$\begin{aligned} g_u(z) &= \sum_{v=(v_1,\ldots,v_s) \in \mathbb{F}_q^n} \zeta^{T((u_1,v_1))+\cdots+T((u_s,v_s))} z^{\delta_1(v_1)+\cdots+\delta_s(v_s)} \\ &= \prod_{i=1}^{s} \left(\sum_{v_i \in \mathbb{F}_q^{n_i}} \zeta^{T((u_i,v_i))} z^{\delta_i(v_i)} \right), \end{aligned}$$

where

$$\delta_i(v_i) = \begin{cases} 0 & \text{if } v_i = 0 \in \mathbb{F}_q^{n_i}, \\ 1 & \text{otherwise.} \end{cases}$$

It is easy to see that

$$\sum_{v_i \in \mathbb{F}_q^{n_i}} \zeta^{T((u_i,v_i))} z^{\delta_i(v_i)} = \begin{cases} 1 + (q^{n_i} - 1)z & \text{if } u_i = 0 \in \mathbb{F}_q^{n_i}, \\ 1 - z & \text{otherwise.} \end{cases}$$

If $n_1 = n_2 = \cdots = n_s = m$, then the formula for $g_u(z)$ becomes

$$g_u(z) = (1 + (q^m - 1)z)^{s - w_\pi(u)}(1 - z)^{w_\pi(u)}.$$

Therefore by (7) it follows that

$$q^k \sum_{v \in C^\perp} z^{w_\pi(v)} = \sum_{u \in C} g_u(z) = \sum_{u \in C} (1 + (q^m - 1)z)^{s - w_\pi(u)}(1 - z)^{w_\pi(u)}.$$

Thus we have the following MacWilliams Identity:

Theorem 4.3. *Let C be a linear code over $\mathbb{F}_q$ with type $\pi = [m]^s$. Then*

$$f_{C^\perp}(x, y) = \frac{1}{|C|} f_C(x + (q^m - 1)y, x - y).$$

As an application of the weight enumerator, we have the following result:

Theorem 4.4. *For a MDS linear code $C = [n, k, d]_q$ with type $[m]^s$ where $n = ms$, $k = (s - d + 1)m$, $(1 \leqslant d \leqslant s - 1)$, we have $s + 2 - q^m \leqslant d \leqslant q^m$.*

Proof. As in the classical case, for any MDS linear code $C = [n, k, d]_q$ with type $[m]^s$, the weight enumerator $f_C(x, y) = \sum_{i=0}^{s} A_i x^{s-i} y^i$ of C is determined by n, k and d:

$$A_i = \binom{s}{i} (q^m - 1) \sum_{j=0}^{i-d} \binom{i-1}{j} q^{m(i-d-j)}(-1)^j \quad (d \leqslant i \leqslant s).$$

By the assumption that $d \leqslant s - 1$, we obtain that

$$0 \leqslant A_{d+1} = \binom{s}{d+1} (q^m - 1)(q^m - d).$$

Therefore $d \leqslant q^m$. Then considering the dual MDS code $C^\perp = [n, n - k, d^\perp]_q$, we get $q^m \geqslant d^\perp = s - d + 2$, which means that $d \geqslant s + 2 - q^m$. □

5. Algebraic-geometry codes

Algebraic-geometry (AG) codes, introduced by Goppa, is a powerful class of classical codes that can be generalized directly to the error-block case. This section uses the following notations:

$F/\mathbb{F}_q$: function field with constant field $\mathbb{F}_q$.
$g = g(F)$: the genus of F.
$D(F)$: the group of divisors of F.
$\deg A$: the degree of a divisor $A \in D(F)$.
$\Omega = \Omega(F)$: the space of differential of F.
$\mathrm{div}(f)$: the divisor of a function $0 \neq f \in F$.
$W = \mathrm{div}(\omega)$: the divisor of a differential $\omega \in \Omega$.
$\mathrm{res}_{\mathcal{P}}(\omega)$: the residue of a differential ω at a prime divisor $\mathcal{P}$.

$L(A) = \{f \in F | \mathrm{div}(f) \geqslant -A\}$ for $A \in D(F)$.
$\Omega(A) = \{\omega \in \Omega | \mathrm{div}(\omega) \geqslant A\}$ for $A \in D(F)$.
$l(A) = \dim_{\mathbb{F}_q} L(A)$.
$d(A) = \dim_{\mathbb{F}_q} \Omega(A)$.
$v_{\mathcal{P}} : F \to \mathbb{Z} \cup \infty$: the normalized $\mathcal{P}$-adic exponential valuation of F at a prime divisor $\mathcal{P}$.

Lemma 5.1 (*Riemann–Roch Theorem*). *For a divisor $A \in D(F)$, we have $l(A) = \deg A + 1 - g + d(A)$, $d(A) = l(W - A)$.*

Lemma 5.2. *For a prime divisor $\mathcal{P}$ of degree d, let $T_{\mathcal{P}}$ be the trace mapping for $\mathbb{F}_{q^d}/\mathbb{F}_q$. Then for each $\omega \in \Omega$, we have $\sum_{\mathcal{P}} T_{\mathcal{P}}(\mathrm{res}_{\mathcal{P}}(\omega)) = 0$.*

Let $n = n_1 + n_2 + \cdots + n_s$, and $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \oplus \cdots \oplus \mathbb{F}_q^{n_s}$. For $m \geqslant 1$ and any fixed $\mathbb{F}_q$-basis $\{\alpha_1, \ldots, \alpha_m\}$ of $\mathbb{F}_{q^m}$, we have the $\mathbb{F}_q$-linear isomorphism

$$\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m, \quad c = c_1\alpha_1 + \cdots + c_m\alpha_m \to (c_1, \ldots, c_m) \quad (c_i \in \mathbb{F}_q).$$

We identify an element $c \in \mathbb{F}_{q^m}$ with the vector $(c_1, \ldots, c_m) \in \mathbb{F}_q^m$, so that $\mathbb{F}_q^n = \mathbb{F}_{q^{n_1}} \oplus \cdots \oplus \mathbb{F}_{q^{n_s}}$.

Theorem 5.3. *Let $F/\mathbb{F}_q$ be a function field, and $g = g(F)$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_s$ be distinct prime divisors of F such that $\deg \mathcal{P}_i = n_i$ $(1 \leqslant i \leqslant s)$, $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s$, $n = n_1 + n_2 + \cdots + n_s$, $D = \mathcal{P}_1 + \mathcal{P}_2 + \cdots + \mathcal{P}_s$. Let G be an effective divisor of F ("effective" means that $G = \sum_{\mathcal{P}} v_{\mathcal{P}}(G)\mathcal{P}$ and $v_{\mathcal{P}}(G) \geqslant 0$ for all prime divisor $\mathcal{P}$) and $v_{\mathcal{P}_i}(G) = 0$ $(1 \leqslant i \leqslant s)$.*

(i) *Assuming that $\deg G \leqslant n - 1$, it follows that*

$$C(D, G) = \{c_f = (f(\mathcal{P}_1), \ldots, f(\mathcal{P}_s)) | f \in L(G)\}$$

is a linear code $[n, k, d]_q$ with type $\pi = [n_1][n_2]\ldots[n_s]$ where $k = l(G) \geqslant \deg G + 1 - g$, $d \geqslant t$ and t is determined by

$$n_s + n_{s-1} + \cdots + n_{t+1} - 1 < \deg G \leqslant n_s + n_{s-1} + \cdots + n_t - 1.$$

Moreover, $k = \deg G + 1 - g$ if $\deg G \geqslant 2g - 1$, and $d = t$ if $n_s + n_{s-1} + \cdots + n_{t+1} - 1 + g < \deg G$.

(ii) *Assuming that $\deg G \geqslant 2g - 1$, it follows that*

$$C'(D, G) = \{c_\omega = (\mathrm{res}_{\mathcal{P}_1}\omega, \ldots, \mathrm{res}_{\mathcal{P}_s}\omega) | \omega \in \Omega(G - D)\}$$

is a linear code $[n, k', d']_q$ with type $\pi = [n_1][n_2]\ldots[n_s]$ where $k' = d(G - D) \geqslant n - \deg G + g - 1$, $d' \geqslant t'$, and t' is determined by

$$n_1 + n_2 + \cdots + n_{t'-1} + 2g - 1 \leqslant \deg G < n_1 + n_2 + \cdots + n_{t'} + 2g - 1.$$

Moreover, $k' = \deg G + g - 1$ if $\deg G \leqslant n - 1$, and $d' = t'$ if $n_1 + \cdots + n_{t'} - 1 + g > \deg G$.

(iii) *For each* i, $1 \leqslant i \leqslant s$, *we choose* $\{\alpha_1^{(i)}, \ldots, \alpha_{n_i}^{(i)}\}$ *and* $\{\alpha_1^{(i)'}, \ldots, \alpha_{n_i}^{(i)'}\}$ *to be trace-dual bases for* $\mathbb{F}_{q^{n_i}}/\mathbb{F}_q$. *This means that*

$$T_{\mathcal{P}_i}(\alpha_\lambda \alpha'_\mu) = \delta_{\lambda\mu} = \begin{cases} 1 & \text{if } \lambda = \mu, \\ 0 & \text{if } \lambda \neq \mu, \end{cases}$$

where $1 \leqslant \lambda, \mu \leqslant n_i$, *and* $T_{\mathcal{P}_i}$ *is the trace mapping for* $\mathbb{F}_{q^{n_i}}/\mathbb{F}_q$. *For* $c_f = (f(\mathcal{P}_1), \ldots, f(\mathcal{P}_s)) \in C(D, G)$, $f(\mathcal{P}_i) = \sum_{\lambda=1}^{n_i} a_\lambda^{(i)} \alpha_\lambda^{(i)}$ $(a_\lambda^{(i)} \in \mathbb{F}_q)$, *we identify* $f(\mathcal{P}_i)$ *with* $v^{(i)} = (a_1^{(i)}, \ldots, a_{n_i}^{(i)}) \in \mathbb{F}_q^{n_i}$ *and* $c_f = (v^{(1)}, \ldots, v^{(s)}) \in \mathbb{F}_q^n$. *Similarly, for* $c_\omega = (\mathrm{res}_{\mathcal{P}_1}\omega, \ldots, \mathrm{res}_{\mathcal{P}_s}\omega) \in C'(D, G)$ *and* $\mathrm{res}_{\mathcal{P}_i}\omega = \sum_{\lambda=1}^{n_i} a_\lambda^{(i)'} \alpha_\lambda^{(i)'}$ $(a_\lambda^{(i)'} \in \mathbb{F}_q)$, *we identify* $\mathrm{res}_{\mathcal{P}_i}\omega$ *with* $v^{(i)'} = (a_1^{(i)'}, \ldots, a_{n_i}^{(i)'}) \in \mathbb{F}_q^{n_i}$ *and* $c_\omega = (v^{(1)'}, \ldots, v^{(s)'}) \in \mathbb{F}_q^n$. *Then* $C(D, G)^\perp = C'(D, G)$ *provided that* $2g - 1 \leqslant \deg G \leqslant n - 1$.

Proof. To prove (i) let $C(D, G) = \mathrm{im}(\varphi)$ where φ is the $\mathbb{F}_q$-linear mapping:

$$\varphi : L(G) \to \oplus_{i=1}^s \mathbb{F}_{q^{n_i}} = \mathbb{F}_q^n, \quad f \to c_f = (f(\mathcal{P}_1), \ldots, f(\mathcal{P}_s)).$$

For each $f \in L(G)$,

$$\begin{aligned} f \in \ker\varphi &\iff f(\mathcal{P}_i) = 0 \quad (1 \leqslant i \leqslant s) \\ &\iff f \in L(G - D) \quad (D = \mathcal{P}_1 + \cdots + \mathcal{P}_s). \end{aligned}$$

Since $\deg(G - D) = \deg G - \deg D = \deg G - n < 0$, it follows that $L(G - D) = 0$, so that $\ker\varphi = (0)$. Thus

$$\begin{aligned} k &= \dim_{\mathbb{F}_q} C(D, G) = \dim_{\mathbb{F}_q} L(G) = l(G) \\ &= \deg G + 1 - g + l(W - G) \quad \text{(by Lemma 5.1)} \\ &\geqslant \deg G + 1 - g. \end{aligned}$$

Moreover, if $\deg G \geqslant 2g-1$ then $\deg(W-G) = 2g-2-\deg G < 0$, so that $l(W-G) = 0$ and $k = \deg G + 1 - g$.

Now we estimate d. Suppose that there exists $c_f \in C(D, G)$ $(f \in L(G))$ such that $w_\pi(c_f) \leqslant t - 1$. Then c_f has at least $s - t + 1$ zero block-components:

$$f(\mathcal{P}_{i_\lambda}) = 0 \quad (1 \leqslant \lambda \leqslant s - t + 1), \quad 1 \leqslant i_1 < i_2 < \cdots < i_{s-t+1} \leqslant s.$$

Thus $f \in L(G-(\mathcal{P}_{i_1}+\cdots+\mathcal{P}_{i_{s-t+1}}))$. By the assumption $\deg G \leqslant n_s+n_{s-1}+\cdots+n_t-1$, it follows that $\deg(G - (P_{i_1} + \cdots + P_{i_{s-t+1}})) = \deg G - \sum_{j=1}^{s-t+1} n_{i_j} \leqslant \deg G - (n_s + n_{s+1} + \cdots + n_t) < 0$. Thus $f = 0$ and $c_f = 0$. Therefore, $d \geqslant t$. Moreover, if $\deg G > n_s + n_{s+1} + \cdots + n_{t+1} - 1 + g$, then

$$l(G - (\mathcal{P}_s + \mathcal{P}_{s-1} + \cdots + \mathcal{P}_{t+1})) \geqslant \deg G - (n_s + n_{s-1} + \cdots + n_{t+1}) + 1 - g \geqslant 1.$$

Thus there exists $0 \neq f \in L(G - (\mathcal{P}_s + \mathcal{P}_{s-1} + \cdots + \mathcal{P}_{t+1})) \subseteq L(G)$, such that $1 \leqslant w_\pi(c_f) \leqslant t$. Therefore $d = t$.

To prove (ii) note that $C'(D,G) = \operatorname{im}\varphi'$ where φ' is the $\mathbb{F}_q$-linear mapping

$$\varphi' : \Omega(G-D) \to \oplus_{i=1}^{s}\mathbb{F}_{q^{n_i}} = \mathbb{F}_q^n, \quad \omega \to (\operatorname{res}_{\mathcal{P}_1}\omega, \ldots, \operatorname{res}_{\mathcal{P}_s}\omega).$$

For each $\omega \in \Omega(G-D)$,

$$\omega \in \ker\varphi' \Longleftrightarrow \operatorname{res}_{\mathcal{P}_i}\omega = 0 \in \mathbb{F}_{q^{n_i}} \quad (1 \leqslant i \leqslant n) \Longleftrightarrow \omega \in \Omega(G).$$

Since $\deg(\operatorname{div}\omega) = 2g-2$ for any $0 \neq \omega \in \Omega$, we know that $\Omega(G) = (0)$ by assumption $\deg G \geqslant 2g-1$. Therefore $\ker\varphi' = (0)$ and

$$\begin{aligned} k' &= \dim_{\mathbb{F}_q}\Omega(G-D) = d(G-D) = l(W+D-G) \\ &= \deg(W+D-G) + 1 - g + l(G-D) \\ &= n - \deg G + g - 1 + l(G-D) \\ &\geqslant n - \deg G + g - 1. \end{aligned}$$

Moreover, if $\deg G \leqslant n-1$, then $\deg(G-D) < 0$ and $l(G-D) = 0$, so that $k' = n - \deg G + g - 1$.

Now we estimate d'. Suppose that there exists $c_\omega \in C'(D,G)(\omega \in \Omega(G-D))$ such that $w_\pi(c_\omega) \leqslant t'-1$. Then $\operatorname{res}_{\mathcal{P}_i}\omega = 0$ $(i \in S)$ for some subset S of $\{1,2,\ldots,s\}$, $|S| = s - t' + 1$. Thus $\omega \in \Omega(G - \sum_{i=1, i\notin S}^{s}\mathcal{P}_i)$. By the assumption that $\deg G \geqslant n_1 + n_2 + \cdots + n_{t'-1} + 2g - 1$, it follows that

$$\deg\left(G - \sum_{i=1, i\notin S}\mathcal{P}_i\right) \geqslant \deg G - (n_1 + n_2 + \cdots + n_{t'-1}) > 2g-2.$$

Thus $\Omega\left(G - \sum_{i=1, i\notin S}^{s}\mathcal{P}_i\right) = (0)$ so that $\omega = 0$ and $c_\omega = 0$. Therefore $d' \geqslant t'$. Moreover, if $\deg G < n_1 + n_2 + \cdots + n_{t'} + g - 1$, then

$$d\left(G - \sum_{i=1}^{t'}\mathcal{P}_i\right) = \sum_{i=1}^{t'} n_i - \deg G + g - 1 + l\left(G - \sum_{i=1}^{t'}\mathcal{P}_i\right) \geqslant 1.$$

Thus there exists $0 \neq \omega \in \Omega(G - \sum_{i=1}^{t'}\mathcal{P}_i) \subseteq \Omega(G-D)$ such that $1 \leqslant w_\pi(c_\omega) \leqslant t'$. Therefore $d' = t'$.

To prove (iii) note that under the assumption $2g-1 \leqslant \deg G \leqslant n-1$, it follows that

$$C(D,G) = [n,k,d]_q, \quad C'(D,G) = [n,k',d']_q,$$

where $k = \deg G + 1 - g, k' = n - \deg G + g - 1 = n - k$. For each i $(1 \leqslant i \leqslant s)$ it follows that

$$f(\mathcal{P}_i) = \sum_{\lambda=1}^{n_i} a_\lambda^{(i)}\alpha_\lambda^{(i)} \in \mathbb{F}_{q^{n_i}} \quad (a_\lambda^{(i)} \in \mathbb{F}_q),$$

$$\operatorname{res}_{\mathcal{P}_i}\omega = \sum_{\lambda=1}^{n_i} a_\lambda^{(i)'}\alpha_\lambda^{(i)'} \in \mathbb{F}_{q^{n_i}} \quad (a_\lambda^{(i)'} \in \mathbb{F}_q)$$

and so

$$T_{\mathcal{P}_i}(f(\mathcal{P}_i)\mathrm{res}_{\mathcal{P}_i}\omega) = T_{\mathcal{P}_i}\left(\sum_{\lambda,\mu=1}^{n_i} a_\lambda^{(i)}\alpha_\lambda^{(i)}a_\mu^{(i)'}\alpha_\mu^{(i)'}\right)$$

$$= \sum_{\lambda=1}^{n_i} a_\lambda^{(i)}a_\lambda^{(i)'} \in \mathbb{F}_q.$$

For any $c_f \in C(D,G)$ and $c_\omega \in C'(D,G)$ where $f \in L(G), \omega \in \Omega(G-D)$, then $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) \geqslant -G + G - D = -D$. Thus $\mathrm{res}_{\mathcal{P}}(f\omega) = 0$ for any prime divisor $\mathcal{P} \notin \{\mathcal{P}_1, \ldots, \mathcal{P}_s\}$. By Lemma 5.2, we have

$$0 = \sum_{\mathcal{P}} T_{\mathcal{P}}(\mathrm{res}_{\mathcal{P}} f\omega) = \sum_{i=1}^{s} T_{\mathcal{P}_i}(f(\mathcal{P}_i)\mathrm{res}_{\mathcal{P}_i}\omega)$$

$$= \sum_{i=1}^{s}\sum_{\lambda=1}^{n_i} a_\lambda^{(i)}a_\lambda^{(i)'} = (c_f, c_\omega).$$

This completes the proof that $C(D,G)^\perp = C'(D,G)$. □

Example. We consider $F = \mathbb{F}_q(x)$. In this case, $g = 0$, the number $N_q(d)$ of prime divisors with degree d in $\mathbb{F}_q(x)$ is

$$N_q(1) = q + 1, \quad (\mathcal{P} = (x-a), a \in \mathbb{F}_q \text{ and } \mathcal{P} = \infty)$$

$$N_q(d) = \frac{1}{d}\sum_{e|d} \mu(e) q^{d/e} \quad (\text{for } d \geqslant 2)$$

$$= \sharp\{\text{monic irreducible polynomials of degree } d \text{ in } \mathbb{F}_q[x]\}.$$

As a direct consequence of Theorem 5.3, we obtain the first result in the following theorem. The second result comes from Theorem 2.3.

Theorem 5.4. *Let* $\pi = [n_1]\ldots[n_s] = [m_1]^{l_1}\ldots[m_t]^{l_t}$ *where* $n_1 \geqslant n_2 \geqslant n_s$, $m_1 > m_2 > m_t \geqslant 1$, $n = \sum_{i=1}^{s} n_i = \sum_{j=1}^{t} l_j m_j$, $1 \leqslant l_j \leqslant N_q(m_j)$ $(1 \leqslant j \leqslant t)$.

(i) *For each* k, $1 \leqslant k \leqslant n$, *there exists linear code* $C = [n,k,d]_q$ *with type* π *where* d *is determined by*

$$n_s + n_{s-1} + \cdots + n_{d+1} < k \leqslant n_s + n_{s-1} + \cdots + n_d.$$

In particular, C *is an MDS code if* $k = n_s + n_{s-1} + \cdots + n_d$.

(ii) *Suppose that* $s \geqslant 3$ *and* $n_1 + n_2 \leqslant n - k < n_1 + n_2 + n_3$. *Then* $N = \frac{q^{n-k}-1}{q-1} - \sum_{i=1}^{s} \frac{q^{n_i}-1}{q-1} \geqslant 0$, *and there exists linear code* $C = [n + r, k + r, 3]_q$ *with type* $[n_1] \ldots [n_s][1]^r$ *provided* $0 \leqslant r \leqslant N$. *Moreover, C is a perfect code if* $r = N$.

6. Conclusion and open problems

This paper presents several algebraic methods to construct good linear error-block codes as direct analogies of the classical case. Many problems remain for further research. Several of them are mentioned here.

1. Determining all perfect codes may be a big problem even for restricted types, such as the classical case ($\pi = [1]^n, n \geqslant 1$). However, we may pose some subproblems: How does one construct perfect codes with $d > 3$ and type $\neq [1]^n$? Is the number of perfect codes with type $[n_1][1]^{s-1}$ (n_1 is fixed and $s \geqslant 1$) finite except obvious series?
2. Since a general partition of $\{1, 2, \ldots, n\}$ may have different sizes of components n_i $(1 \leqslant i \leqslant s)$, cyclic codes can not be generalized to the error-block case directly. But, using the zeros of (the generating polynomial of) a cyclic code, we may construct cyclic codes with type $\pi \neq [1]^n$ having larger minimal distance d like BCH codes. On the other hand, the weight enumerator of irreducible cyclic codes can be calculated by using computation of Gauss sums. This can be done for more general type with proper partition of coordinates $\{1, 2, \ldots, n\}$.
3. Find new ways to construct nice error-block codes. For example, it appears that some new versions of AG codes, such as the XNL codes in [9] can be generalized to the error-block case.
4. Find relations of error-block codes to combinatorial designs, finite geometry and other combinatorial structures. Can the minimal weight codewords of some error-block codes form new type of combinatorial design? Construct error-block codes by using finite geometry and research their symmetry properties.
5. We may consider the relationships of error-block codes for different partitions of $\{1, 2, \ldots, n\}$. This is another combinatorial aspect of error-block codes. All partitions of $\{1, 2, \ldots, n\}$ form a partially ordered set (Poset) by defining $\pi \preccurlyeq \pi'$ to mean that each component of π' is a union of one or more components of π. If C is a linear code $[n, k, d]_q$ with type π', then C is also a code $[n, k, d]_q$ with type π for any $\pi \preccurlyeq \pi'$. For fixed q, n, k and d, let $\mathcal{P} = \mathcal{P}_q(n, k, d)$ be the set of partitions π of $\{1, 2, \ldots, n\}$ such that there exists a linear code $[n, k, d]_q$ with type π. How does one describe the set of maximum elements of $\mathcal{P}$?
6. Construct tables of parameters for "optimal" error-block codes. Since the type π is related to n, there are many ways to judge the optimality of a code. One simple way is to ask that for fixed n, q and type π, how the parameters k and d are related?
7. Research non-linear error-block codes.

Acknowledgements

A part of this work carried out while K. Feng was visiting the Hong Kong Baptist University invited by Professor Fred J. Hickernell. He gratefully acknowledges HKBU for hospitality during this visit.

References

[1] R. Brualdi, J.S. Graves, M. Lawrence, Codes with a poset metric, Discrete Math. 147 (1995) 57–72.
[3] A.S. Hedayat, N.J.A. Sloane, J. Stufken, Orthogonal Arrays: Theory and Applications, Springer Series in Statistics, Springer, New York, 1999.
[4] J.Y. Hyun, H.K. Kim, The poset structures which admit the extended binary Hamming code to be a perfect code, preprint, 2002.
[5] Y. Lee, Projective systems and perfect codes with a poset metric, Finite Fields Appl. 10 (2004) 105–112.
[6] J.H. van Lint, Introduction to Coding Theory, third ed., Graduate Texts in Mathematics, vol. 86, Springer, Berlin, 1999.
[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier Science, Amsterdam, 1988.
[8] H. Niederreiter, Points sets and sequences with small discrepancy, Monatsh. Math. 104 (1987) 221–228.
[9] H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields, London Mathematical Society Lecture Note Series, vol. 285, Cambridge University Press, Cambridge, 2001.